

Exhibit 4

In Search of Shadows: Investigating and Prosecuting Crime on the “Dark Web”

Keith Becker
Deputy Chief
Child Exploitation and Obscenity Section

Ben Fitzpatrick
Senior Counsel
Computer Crime and Intellectual Property Section

Technologically sophisticated offenders deploy a multitude of strategies to perpetrate online-facilitated crimes without getting caught. This article will discuss common technological and legal challenges presented when investigating and prosecuting criminals who use the so-called “Dark Web.”

I. What is the “Dark Web”

Consider the internet in three related parts, commonly depicted as an iceberg with some part of the structure above the water’s surface and a larger part below: *first*, above the water line is the “Open Internet,” that is, publicly-accessible web pages that can be “crawled” or “indexed” by search engines such as Google so that internet users may search for content that is contained on those web pages; *second*, below the water line and commonly reported to be the largest portion is the “Deep Web,” that is, web pages whose contents are not crawled or indexed by standard search engines, generally because they are within internal corporate, government, or academic computer networks or behind subscription or pay walls; and *third*, further below is the “Dark Web,” that is, a sub-part of the “Deep Web” consisting of computer networks that require specific software or software configurations to access.

A. What Does the Dark Web Allow Users to Do

The primary feature of a Dark Web computer network is that it allows users to communicate over the internet anonymously. Dark Web networks offer all of the same kinds of communication platforms as the open internet—websites, chat, file sharing, etc.—with the added benefit of robust anonymity. The most popular Dark Web network—and unsurprisingly, one that factors into numerous law enforcement investigations—is the Tor network.

II. What is the Tor Network

The Tor network is designed to provide anonymity to users by encrypting and then routing online communications through a network of relay computers run by volunteers all around the world. This prevents the end recipients of communications from learning a user’s internet protocol address (IP address), which could otherwise be used to identify a user. Originally created by the United States Naval Research Laboratory to protect government communications, it is currently run and maintained by the nonprofit Tor Project. To access the Tor network, a user must install Tor software, which is most easily accomplished by downloading the free “Tor browser,” a version of the “Mozilla Firefox” web browser

that is pre-configured to communicate via the Tor network. Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at www.torproject.org.

A. How Does Tor Provide Anonymity

Tor software provides for user anonymity in two primary ways: *first*, by allowing Tor users to access ordinary “Open Internet” websites without revealing their IP addresses to the website; and *second*, by allowing users to operate (and access) Dark Web websites, called “hidden services,” whose actual server location is obscured.

Let’s first examine Tor’s use for anonymous internet communications. Ordinarily, when an individual accesses a website (such as www.justice.gov), that user’s IP address information is transmitted to the website’s computer server (a “web server”) and recorded in the server’s logs. Using legal process, investigators can obtain those logs and then compel an internet service provider to disclose basic subscriber information about the customer to which a pertinent IP address was assigned—information that is critical to trace internet communications to specific devices and individuals.

When a person uses Tor to access the same ordinary internet website, however, communications between the Tor user’s computer and the web server are routed through a series of intermediary computers. As a result, only the IP address of the last computer through which the Tor user’s communications were routed (which is known as the “exit node”) is revealed to, and recorded by, the web server. Thus, any IP address logs on that web server would not contain the actual IP address of a Tor user’s computer. By masking a Tor user’s true IP address, Tor effectively conceals the actual location of Tor users’ computers. A criminal suspect’s use of Tor accordingly makes it extremely difficult, if not impossible, for law enforcement agents who are investigating online crime to determine a Tor user’s physical location.

In addition to providing a means for users to access the internet without revealing their true IP addresses, Tor also makes it possible for users to operate and use websites—which Tor calls “hidden services”—on the Dark Web. Like ordinary internet websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services bear unique technical features that conceal the computer server’s location.

In the case of an ordinary internet website (such as www.justice.gov), a publicly available query can be performed, via a Domain Name System (DNS) listing, to determine the IP address of the computer server that hosts the website. Further publicly available queries may be run regarding that IP address to determine the owner and location of the computer server. Legal process may then be served on the owner or operator of that computer server in order to lawfully obtain information about, or the contents of, that computer server.

As distinguished from an ordinary internet web address (such as www.justice.gov), a Tor-based web address is comprised of a series of sixteen algorithm-generated characters, such as “asdlk8fs9dfiku7f,” followed by the suffix “.onion.” Unlike ordinary internet websites, there is no publicly available query that may be performed via a DNS listing to determine the IP address of the computer server that hosts a Tor hidden service. Moreover, communications between users’ computers and a Tor hidden service web server are routed—as with all Tor communications—through a series of intermediary computers. Accordingly, neither law enforcement nor hidden service users can determine the true IP address—and therefore the location—of the computer server that hosts a hidden service through public lookups or ordinary investigative means. Such a website can effectively be hosted anywhere in the world without accountability to any government or law.

III. How Do Criminals Exploit the Dark Web

Unsurprisingly, criminals take full advantage of the anonymity afforded by Tor and other anonymous services to engage in a wide variety of illegal activity, for example, to hide their identity while perpetrating crimes such as swatting (falsified calls to emergency services made to generate a police response), cyberstalking (use of the internet to harass a victim), or sextortion (an attempt to extort sexually explicit images from a victim, usually via threat to disseminate other such images), and to access internet e-mail, social networking, or other online accounts without leaving an identifiable trail.

A. What Technologies Do Offenders Use to Maintain Anonymity

Anonymous networks like Tor make up only one type of technologically sophisticated, online tool that criminals can deploy in order to avoid detection by law enforcement. Virtual Private Networks (“VPN”), proxy servers, anonymous e-mail providers, and other web services that neither retain nor provide any identifying information in response to lawful legal process can make it virtually impossible for law enforcement to track down the identity and location of criminal suspects. End-to-end encrypted communication channels provide another mechanism for online criminals to ensure that, even with appropriate court-authorization, law enforcement agencies cannot surveil communications regarding ongoing criminal schemes. Furthermore, the ever-more widespread use of virtual currencies and secondary services that help launder illicit proceeds create significant challenges to tracing illicit payments. Foremost among them is the difficulty in obtaining records from the virtual currency operators that could help investigators conclusively identify the participants in a criminal transaction, as well as the difficulty in tracing transactions made with virtual currencies.

Compounding the investigative problems inherent in these anonymizing technologies is the global and borderless nature of all internet-facilitated crime—which means not only that evidence may be located on computer servers anywhere in the world, but also that criminal actors may engage in a so-called race to the bottom—seeking out web hosting services or other online platforms in jurisdictions perceived to be beyond law enforcement’s reach. A significant challenge that this causes is that to obtain evidence located abroad, United States law enforcement may have to rely on the criminal laws of other countries and an often-cumbersome mutual legal assistance treaty (MLAT) process, which too often does not operate at the speed needed to effectively investigate cybercrime.

B. What Unique Problem is Posed by Tor Hidden Services

Fully anonymous platforms such as Tor hidden services, however, pose a unique and significant threat to public safety. In that environment, offenders set up websites exclusively dedicated to criminal aims that operate openly and notoriously. Law enforcement agents can access the sites and document the content and criminal activity taking place, but are unable to utilize the sort of investigative steps—a combination of publicly available queries and legal process—that would ordinarily allow them to timely determine where the crimes are occurring and who is perpetrating them. The fact that law enforcement can generally identify evidence and perpetrators when crimes occur via ordinary internet websites deters offenders from engaging in open and notorious criminal activity via the internet. Absent that crucial deterrence effect, criminal hidden services stabilize and grow.

This phenomenon is perhaps most evident in the persistent problem of criminal child exploitation communities that operate via Tor hidden services, where like-minded child sex offenders gather to promote and normalize the sexual abuse of children, educate each other about how to perpetrate child sex abuse without getting caught, and share images and videos depicting the sexual abuse and exploitation of children as young as infants and toddlers. Such communities are disturbingly commonplace and frequently involve tens of thousands of members. In addition, so-called Dark Markets—where offenders may buy, sell and trade illicit goods such as narcotics, firearms, credit card numbers, hacking tools and ill-gotten, personally identifying information in an environment that protects the anonymity of criminal

sellers and purchasers—also abound. In the midst of an opioid crisis occurring in the United States, the open availability of Dark Markets, where illicit narcotics are freely available, poses a significant public health threat.

Anonymizing technology like Tor software not only provides criminals with a platform on which to conduct criminal activity, but also with a tool to undermine law enforcement’s ability to investigate that activity, identify and apprehend perpetrators, and rescue victims.

IV. What Strategies Can Be Employed to Meet These Challenges

Combating offenders’ use of sophisticated techniques to hide their identity and location requires a multi-faceted approach. The global nature of online-facilitated crime in general, and sophisticated online crimes in particular, means that law enforcement must frequently collaborate with international partners to determine where criminal activity is occurring, as well as how evidence and criminal infrastructure can be seized so that perpetrators can be brought to justice. In recent years, coalitions of United States and foreign law enforcement agencies, frequently led by the Department of Justice, have seized numerous dark markets and other criminal facilities that rely on virtual currency to operate. In July 2017, for example, the Department announced a multinational effort that dismantled Alpha Bay, the largest criminal dark market then in operation. In February 2015, the FBI launched Operation Pacifier, discussed herein, which successfully interdicted a global child exploitation network. These operations followed the success of Operation Onymous, an international takedown in November 2014 of dozens of dark market websites, including the successor site to Silk Road (an online illicit drug marketplace), which itself was seized in October 2013.

Criminals’ use of advanced technology to obscure the identity and location of perpetrators and evidence means that law enforcement agencies must employ a variety of strategies—both ordinary and technical—to find and obtain evidence and identify and apprehend perpetrators. Even sophisticated criminals sometimes make mistakes. Determined, old-fashioned detective work may, in some instances, discover an error in a network or browser configuration that exposes the actual location of a Dark Web website or a clue that leads investigators to the actual identity of a perpetrator otherwise acting under an online alias. At the other end of the spectrum, investigators may be able to develop and deploy advanced tools and techniques that counteract criminals’ use of sophisticated technology, such as network investigative techniques (NITs), which can pierce the veil of anonymity offered by networks such as Tor and provide investigators with crucial, user-attributable information such as IP addresses.

In addition, legal authorities must be appropriately adapted to new and emerging technologies to ensure that advanced criminal schemes do not outpace the ability of law enforcement to appropriately utilize legal process and, where appropriate, conduct court-authorized searches, seizures or interceptions in order to interdict these schemes. One such adaptation occurred in December 2016, when FED. R. CRIM. P. 41 was amended to specifically authorize a magistrate judge “in any district where activities related to a crime may have occurred”¹ to issue a warrant “to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district” if “the district where the media or information is located has been concealed through technological means.”² This targeted, procedural amendment to the venue provisions of the Rule—which did not alter the probable cause or other Fourth Amendment requirements to obtain a warrant—can help ensure that technologies such as Tor do not render investigative abilities obsolete.

¹ FED. R. CRIM. P. 41(5).

² FED. R. CRIM. P. 41(6).

V. FBI Operation Pacifier

FBI “Operation Pacifier” provides an illustrative example of how law enforcement sought to meet the significant challenges posed by a particular group of offenders’ use of anonymizing technology to perpetrate serious crimes on a massive global scale. “Operation Pacifier” targeted the administrators and users of “Playpen,” a highly-sophisticated, global enterprise dedicated to the sexual exploitation of children, organized via a members-only website that operated as a hidden service on the Tor network. Playpen’s administrators and more than 150,000 other members authored and viewed tens of thousands of postings relating to sexual abuse of children as young as infants and toddlers.

In February 2015, the “Playpen” web server was seized from a web-hosting facility in North Carolina. As noted above, because Playpen was a Tor hidden service, the seizure of the website did not provide law enforcement agents with IP address logs that could be used to identify site users, as well as the children they could have been abusing. Accordingly, it was necessary for the FBI to host, for a brief period, the Playpen website at an FBI facility in the Eastern District of Virginia, during which time the FBI obtained a search warrant to deploy a network investigative technique (“NIT”) and a Title III wiretap order to monitor user communications in an effort to identify those site users and children being victimized by them. The NIT warrant authorized the FBI to deploy the NIT—which consisted of computer code that, when deployed to a user’s computer, caused that computer to send to a government computer its actual IP address as well as a limited set of other, computer-related information—to Playpen users after they logged into the website. After obtaining that basic information via the NIT, additional investigation was conducted in an effort to determine the identity of the persons behind those computers and to search for and seize digital evidence, including the issuance of legal process regarding IP addresses obtained via the NIT and additional search warrants at premises associated with those IP addresses.

The results of the operation have been staggering in the United States and abroad—at least 348 United States arrests, the prosecution of at least fifty-one alleged hands-on child sex abusers, and the identification or rescue of at least fifty-five American children who were subjected to sexual abuse or exploitation; internationally, there have been at least 548 arrests and 296 children identified or rescued from sexual abuse or exploitation.

The Playpen administrators were successfully identified, apprehended and prosecuted as well. On September 16, 2016, a federal jury in the Western District of North Carolina convicted lead site administrator Steven W. Chase, fifty-seven, of Naples, Florida, of engaging in a child exploitation enterprise and related charges, and on May 1, 2017, he was sentenced to thirty years in prison and lifetime supervised release. Chase’s two co-defendants, fellow administrator Michael Fluckiger, forty-six, of Portland, Indiana, and global moderator David Lynn Browning, forty-seven, of Wootton, Kentucky, each pled guilty to engaging in a child exploitation enterprise and were respectively sentenced in January and February of 2017 to twenty years in prison and lifetime supervised release.

The myriad prosecutions related to Operation Pacifier brought to the forefront a number of complex legal issues. Defense strategies have largely focused on three litigation fronts: (1) motions to suppress evidence derived from the court-authorized NIT warrant; (2) motions to compel discovery regarding the investigation, primarily involving NIT “source code”; and (3) motions to dismiss indictments for purported “outrageous government conduct” because the Playpen website briefly operated on a law enforcement server. Although some of these challenges are particular to the scale and complexity of the Pacifier investigation, the strategy employed by defendants in these cases provides insight into the sort of tactics prosecutors can expect to face in other cases that involve anonymous networks and a combination of traditional and technical investigative techniques. While litigation in many cases remains ongoing, to date the government has successfully defended the investigation on all litigation fronts.

The Playpen NIT was deployed before the December 2016 Rule 41 amendment, described above, became effective. As such, many defendants have challenged the warrant authorizing the Playpen NIT, primarily claiming that the issuing magistrate lacked authority to issue it pursuant to the then-existing version of Rule 41, which purportedly rendered the warrant “*void ab initio*” and required suppression of evidence derived from the warrant. To date, three United States Courts of Appeal and more than seventy United States district court orders have denied such challenges, uniformly finding that, at a minimum, suppression of evidence derived from the Playpen NIT warrant is inappropriate under the *Leon* good-faith exception.³ Numerous district courts have also found that the issuing magistrate had proper authority to issue the NIT warrant because it functioned as or similar to a digital tracking device.⁴ The December 2016 Rule 41 amendment—which clarified the circumstances under which a particular magistrate may authorize a remote search of a computer whose location has been concealed through technological means—should largely eliminate such challenges to similar warrants in future investigations.

Some Pacifier defendants have also attempted to compel the government to provide internal Department of Justice or FBI memoranda related to the approval or conduct of the operation, and the computer “source code” related to the NIT. The government has successfully opposed production of that requested information: *first*, by providing substantial discovery to defendants in Pacifier cases (generally subject to protective order) to include IP address and other information collected by the NIT and the actual computer instructions that collected that information; *second*, by challenging the materiality of remaining requests for additional NIT or investigation-related information; and *third*, where appropriate, by contending that certain requested information (largely pertaining to the NIT source code) was subject to various privileges—including the common law “law enforcement privilege.”⁵ Numerous courts have found requests for internal memoranda and NIT source code to be largely based upon a speculative foundation and, therefore, immaterial.⁶ Some courts, in addition to a lack of materiality, have also found “source code” requests properly subject to the law enforcement privilege.⁷

Finally, some Pacifier defendants have moved to dismiss an indictment on the theory that it was so “outrageous” for the FBI to allow the Playpen site to briefly continue operating in order to identify users that any indictment returned against such a user should be dismissed. In response to such allegations, the government has persuasively articulated the justification for the court-authorized effort to

³ To date, all of the district court orders that granted suppression motions regarding the Playpen NIT evidence have been overturned or occurred in a circuit that subsequently ruled suppression to be inappropriate. *See, e.g.*, *United States v. Levin*, 874 F.3d 316, 318 (1st Cir. 2017); *United States of America, v. Yang Kim*, also known as *Andrew Kim*, Defendant., No. 16-CR-191 (PKC), 2017 WL 5256753 at 2 (E.D.N.Y. Nov. 10, 2017) (collecting cases).

⁴ *See United States v. Leonard*, No. 17-CR-135, 2017 WL 4478330 at 3 (E.D. Va. Oct. 6, 2017).

⁵ “The purpose of [the law enforcement privilege] is to prevent disclosure of law enforcement techniques and procedures, to preserve the confidentiality of sources, to protect witness and law enforcement personnel, to safeguard the privacy of individuals involved in an investigation, and otherwise to prevent interference with an investigation.” *In re The City of New York*, 607 F.3d 923, 940-41 (2d Cir. 2010) *quoting In re Dep’t of Investigation of City of New York*, 856 F.2d 481, 484 (2d Cir. 1988); *see also United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987) (noting that the privilege protects against divulging information that would allow criminals to develop countermeasures and techniques that frustrate lawful surveillance). Courts have held that the privilege prevents discovery of sensitive information about technologically sensitive law enforcement techniques and tools, such as NITs. *See United States v. Rigmaiden*, 844 F. Supp. 2d 982, 989, 993-1006 (D. Ariz. 2012) (description of sensitive investigative technologies); *United States v. Piroso*, 787 F.3d 358, 363-67 (6th Cir. 2015) (holding that source code of software used in an investigation is privileged); *United States v. Van Horn*, 789 F.2d 1492, 1507-08 (11th Cir. 1986) (holding that the nature and location of electronic surveillance equipment is privilege).

⁶ *See, e.g.*, *United States v. Zak*, No. 16-CR-65-V, 2017 WL 4358140, 363-65 (W.D.N.Y. Oct. 2, 2017) (denying request for internal memoranda); *United States v. Cruz-Fajardo*, No. 1:16-CR-0014-TCB, 2017 WL 3634278 at 4 (N.D. Ga. Aug. 23, 2017) (denying request for NIT “source code”).

⁷ *See, e.g.*, *United States v. Gaver*, No. 3:16-CR-88, 2017 WL 1134814 at 3 (S.D. Ohio Mar. 27, 2017).

identify sophisticated targets during a brief window of time, while carefully monitoring user communications and appropriately balancing investigative risks and benefits.⁸ No court has granted such a motion.⁹

VI. Conclusion

Technologically sophisticated offenders committing a variety of serious crimes via the Dark Web pose a significant, ongoing, and evolving threat to global public safety and law enforcement. To meet and overcome that threat, law enforcement will have to continue to coordinate globally, develop and deploy both ordinary and technical tools to identify perpetrators and seize evidence, and ensure that legal authorities are updated to prevent criminal schemes from outpacing law enforcement's ability to obtain legal process to further an investigation. If you have questions about Operation Pacifier or criminals' use of the Dark Web to facilitate child exploitation, please feel free to reach out to the Child Exploitation and Obscenity Section (CEOS) in the Criminal Division or your office's Project Safe Childhood (PSC) Coordinator. Other questions about investigating criminal activity on the Dark Web can be directed to the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division or your office's Computer Hacking and Intellectual Property (CHIP) Coordinator. Additional resources regarding the issues discussed herein are available on the Criminal Division intranet.

ABOUT THE AUTHORS

❑ **Keith Becker** is a Deputy Chief with the Criminal Division's Child Exploitation and Obscenity Section (CEOS), where he has worked since 2010. From 2005 to 2010, he served as an Assistant United States Attorney for the District of Columbia, where he prosecuted federal and local cases involving violent crime, narcotics, and child pornography. He has co-authored four other United States Attorneys' Bulletin articles: "Whoever Knowingly Advertises: Considerations in Prosecuting Sex Trafficking," "Child Pornography Conspiracies in the Digital Age: A Primer," "Conspiracy and Internet Technology: Using the Child Exploitation Enterprise Statute to Prosecute Online Child Exploitation," and "Social Networking Site: Breeding Grounds for 'Sextortion' Prosecutions."

❑ **Benjamin Fitzpatrick** is a Senior Counsel in the Computer Crime and Intellectual Property Section of the Criminal Division. Prior to joining CCIPS in 2015, he served as Senior Counsel in the Office of the Deputy Attorney General, working on national security issues, and was a Counsel in the Office of Law & Policy in the National Security Division. Before starting at DOJ in 2012, he was an attorney at Baker Botts, LLP, specializing in litigation and white-collar investigations.

⁸ See *e.g.*, *United States v. Kim*, No. 16-CR-191 (PKC), 2017 WL 394498 at 4 (E.D.N.Y. Jan. 27, 2017).

⁹ See *id.* at 4-7 (collecting cases).